©Akademie d. Wissenschaften Wien; download unter www.biologiezentrum.at

Über ein Theorem des Herrn Pépin.

Von dem c. M. **Leopold Gegenbauer.**

Herr Pépin[1] hat im August 1880 in den Schriften der Pariser Akademie folgenden Satz mitgetheilt:

Die zwei Primzahlen 7 und 13 können nicht Divisoren einer Summe von drei Cuben sein, ohne eine von diesen drei Zahlen zu theilen.

Im September desselben Jahres wurde von Herrn E. Catalon[2] das folgende allgemeine Theorem aufgestellt, welches den die Primzahl 7 betreffenden Theil des Pépin'schen Satzes als speciellen Fall enthält:

Ist p eine ungerade Primzahl und i eine ungerade Zahl des Intervalles $1 \ldots p-1$, so ist die Summe der $\left(\frac{p-1}{2}\right)^{\text{ten}}$ Potenzen von i ganzen zu p theilerfremden Zahlen durch p nicht theilbar.

Ich werde nun in den folgenden Zeilen zunächst einen Satz ableiten, von welchem der auf die Primzahl 13 bezügliche Theil des Pépin'schen Theorems ein specieller Fall ist und sodann ein zweites Theorem derselben Kategorie aufstellen.

Jede reelle Primzahl p von der Form $4\mu+1$ lässt sich bekanntlich nur auf eine einzige Weise in ein Product von zwei conjugirten aus den vierten Einheitswurzeln gebildeten complexen primären Primzahlen $a+bi$ und $a-bi$ zerlegen und es

---

[1] „Sur diverses tentatives de démonstration du théorème de Fermat." Extrait d'une lettre du P. Pépin à M. le Secrétaire perpétuel. Comptes rendus, Tome 91, p. 366—368.

[2] „Sur un théorème de M. Pépin." Mém. soc. roy. d. sciences d. Liège. II. sér. T. 13, p. 291.

©Akademie d

besteht ferner für jede nicht durch p theilbare ganze complexe Zahl α von der Form $\sigma+\tau i$ die Congruenz:

$$\alpha^{\frac{p-1}{4}} \equiv i^{\lambda} \pmod{a+bi}$$

wo λ einen der Werthe 0, 1, 2, 3 besitzt.

Sind nun $a_1, a_2, \ldots, a_r$ r zu p theilerfremde reelle ganze Zahlen, so hat man die Congruenz:

$$\sum_{\rho=1}^{\rho=r} a_\rho^{\frac{p-1}{4}} \equiv \alpha_0 - \alpha_2 + (\alpha_1 - \alpha_3) i \pmod{a+bi}$$

wo α_ν die Anzahl jener Potenzen $a_\rho^{\frac{p-1}{4}}$ ist, welche nach dem Modul $a+bi$ der Einheit i^ν congruent sind, so dass also

$$\alpha_0+\alpha_1+\alpha_2+\alpha_3 = r$$

ist.

Soll nun

$$\sum_{\rho=1}^{\rho=r} a_\rho^{\frac{p-1}{4}} \equiv 0 \pmod{p}$$

sein, so muss

$$\alpha_0 - \alpha_2 + (\alpha_1 - \alpha_3) i \equiv 0 \pmod{a+bi}$$

und daher auch

$$(\alpha_0 - \alpha_2)^2 + (\alpha_1 - \alpha_3)^2 \equiv 0 \pmod{p}$$

sein.

Ist r ungerade, so können nicht beide Differenzen $\alpha_0 - \alpha_2$ und $\alpha_1 - \alpha_3$ gleich Null sein und daher ist die Summe auf der linken Seite der letzten Congruenz sicher zu p theilerfremd, wenn r ungerade und kleiner als $\sqrt{p}$ ist.

Man hat daher den Satz:

Ist p eine Primzahl von der Form $4\mu+1$ und r eine ungerade unterhalb $\sqrt{p}$ befindliche ganze Zahl, so ist die Summe der $\left(\frac{p-1}{4}\right)^{\text{ten}}$ Potenzen von r ganzen zu p theilerfremden Zahlen durch p nicht theilbar.

©Akademie d. Wissenschaften Wien; download unter www.biologiezentrum.at

Für $\mu = 3$ liefert dieses Theorem den auf die Primzahl 13 bezüglichen Theil des Pépin'schen Satzes.

Jede reelle Primzahl p von der Form $6\mu+1$ lässt sich bekanntlich nur auf eine einzige Weise als ein Product von zwei conjugirten aus den dritten Einheitswurzeln ρ gebildeten complexen primären Primzahlen $a+b\rho$ und $a+b\rho^2$ darstellen und es besteht für jede zu p theilerfremde ganze complexe Zahl β von der Form $\sigma+\tau\rho$ die Congruenz:

$$\beta^{\frac{p-1}{3}} \equiv \rho^{\lambda} \pmod{a+b\rho}$$

wo λ einen der Werthe 0, 1, 2 besitzt.

Sind nun $a_1, a_2, \ldots, a_r$ r zu p theilerfremde reelle Zahlen, so ist

$$\sum_{\nu=1}^{\nu=r} a_\nu^{\frac{p-1}{3}} \equiv \beta_0 - \beta_2 + (\beta_1 - \beta_2)\rho \pmod{a+b\rho}$$

wo β_k die Anzahl jener Potenzen $a_\nu^{\frac{p-1}{3}}$ ist, welche nach dem Modul $a+b\rho$ der Einheit ρ^k congruent sind, so dass also

$$\beta_0+\beta_1+\beta_2 = r$$

ist.

Ist nun

$$\sum_{\nu=1}^{\nu=r} a_\nu^{\frac{p-1}{3}} \equiv 0 \pmod{p}$$

so muss auch

$$\beta_0 - \beta_2 + (\beta_1 - \beta_2)\rho \equiv 0 \pmod{a+b\rho}$$

und daher

$$(\beta_0-\beta_2)^2+(\beta_1-\beta_2)^2-(\beta_0-\beta_2)(\beta_1-\beta_2) = sp$$

sein, wo s eine ganze Zahl ist.

Multiplicirt man diese Gleichung mit 4, so verwandelt sich dieselbe in

$$(2\beta_0-\beta_1-\beta_2)^2+3(\beta_1-\beta_2)^2 = 4sp$$

©Akademie d gizentrum.at

oder

$$(3\beta_0 - r)^2 + 3(\beta_1 - \beta_2)^2 = 4sp.$$

Ist nun r nicht durch 3 theilbar, so kann der auf der linken Seite dieser Gleichung stehende Ausdruck nicht verschwinden; derselbe liegt aber auch, wenn r kleiner als $\sqrt{p}$ ist, im Intervalle 1 . . $4p-1$ und daher hat man den Satz:

Ist p eine Primzahl von der Form $6\mu+1$ und r eine nicht durch 3 theilbare, unterhalb $\sqrt{p}$ befindliche ganze Zahl, so ist die Summe der $\left(\frac{p-1}{3}\right)^{\text{ten}}$ Potenzen von r ganzen zu p theilerfremden Zahlen durch p nicht theilbar.

Das von Herrn E. Catalan aufgestellte Theorem und die eben abgeleiteten zwei Sätze kann man in den folgenden Satz zusammenfassen:

Ist λ eine der Zahlen 2, 3, 4, p eine Primzahl von der Form $\lambda\mu+1$ und r eine zu λ theilerfremde unterhalb $p^{\frac{1}{\left[\frac{\lambda+1}{2}\right]}}$ befindliche ganze Zahl, so ist die Summe der $\left(\frac{p-1}{\lambda}\right)^{\text{ten}}$ Potenzen von r zu p theilerfremden ganzen Zahlen durch p nicht theilbar.

Ist p eine reelle Primzahl von der Form $4\mu+1$ und setzt man

$$p = A^2 + B^2 = \mu_1 \cdot \mu_2$$

wo

$$A \equiv 1 \pmod 4$$

ist und μ_1, μ_2 die beiden conjugirten primären Primfactoren von p sind, stellen ferner β'_λ und β''_λ Glieder eines Restensystems nach dem Modul μ_1 vor, welche der Einheit i^λ congruent sind, so ist bekanntlich[1] die Anzahl N der Lösungen der Congruenz:

$$\beta'_0 + \beta_0'' + 1 \equiv 0 \pmod{\mu_1}$$

---

[1] „Bijdrage tot de theorie der derde-en vierde-machtsresten." Door T. J. Stieltjes jr. Versl. en mededeel. d. kon. Akad. v. Wetensch. Amsterdam. Afd. Naturk. II. reeks. XVII. S. 338—417.

für $\mu=2n$ durch die Gleichung

$$8N=4n-3A-5$$

gegeben, während für $\mu=2n+1$ die Relation

$$8N=4n-3A+3$$

besteht.

Da für $n>6$ die beiden für die Anzahl N angegebenen Ausdrücke und überdies für $n=1, 4, 6$ der zweite von ihnen grösser als Null ist, da ferner für $n=1, 3, 4, 6$ im ersten und $n=2, 5$ im zweiten Falle p keine Primzahl ist, so ergibt sich der Satz:

Unter den Primzahlen von der Form $4\mu+1$ haben nur die drei Zahlen 17, 29, 41 die Eigenschaft, niemals Theiler einer Summe von drei zu ihnen theilerfremden Biquadraten zu sein.